Администрирование сетевых подсистем

Лабораторная работа №16

Авдадаев Джамал Геланиевич

11 декабря 2025

Российский университет дружбы народов, Москва, Россия

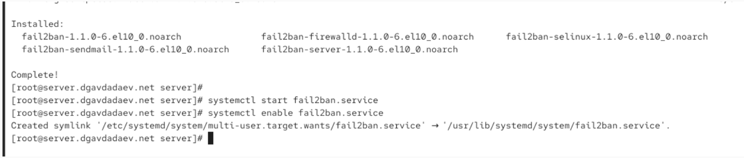
Цели и задачи

Цель лабораторной работы

Получить навыки по настройке Fail2ban для защиты от атак типа «brute force».

Установка и запуск Fail2ban

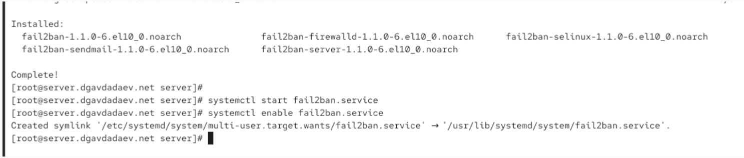
Установка пакета



```
Installed:
  fail2ban-1.1.0-6.el10_0.noarch              fail2ban-firewalld-1.1.0-6.el10_0.noarch      fail2ban-selinux-1.1.0-6.el10_0.noarch
  fail2ban-sendmail-1.1.0-6.el10_0.noarch      fail2ban-server-1.1.0-6.el10_0.noarch

Complete!
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# systemctl start fail2ban.service
[root@server.dgavdadaev.net server]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.dgavdadaev.net server]# █
```

:contentReferenceoaicite:0

Первичный запуск

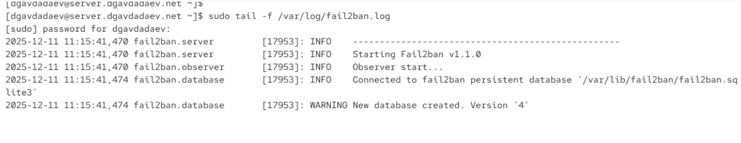


```
Installed:
  fail2ban-1.1.0-6.el10_0.noarch             fail2ban-firewalld-1.1.0-6.el10_0.noarch      fail2ban-selinux-1.1.0-6.el10_0.noarch
  fail2ban-sendmail-1.1.0-6.el10_0.noarch      fail2ban-server-1.1.0-6.el10_0.noarch

Complete!
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# systemctl start fail2ban.service
[root@server.dgavdadaev.net server]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.dgavdadaev.net server]# █
```

:contentReferenceoaicite:1

Первичная проверка работы

Просмотр журнала

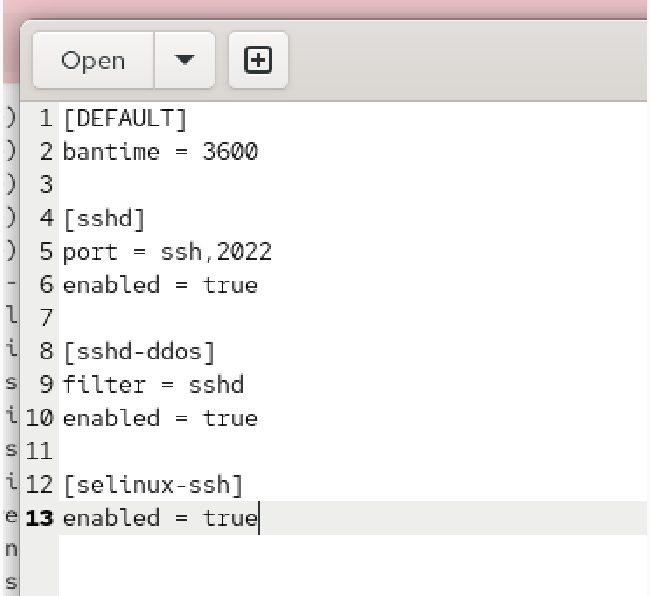


```
[dgavdadaev@server.dgavdadaev.net ~]$
[dgavdadaev@server.dgavdadaev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for dgavdadaev:
2025-12-11 11:15:41,470 fail2ban.server         [17953]: INFO    --------------------------------------------------
2025-12-11 11:15:41,470 fail2ban.server         [17953]: INFO    Starting Fail2ban v1.1.0
2025-12-11 11:15:41,470 fail2ban.observer       [17953]: INFO    Observer start...
2025-12-11 11:15:41,474 fail2ban.database       [17953]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sq
lite3'
2025-12-11 11:15:41,474 fail2ban.database       [17953]: WARNING New database created. Version '4'
```

:contentReferenceoaicite:2

Настройка Fail2ban

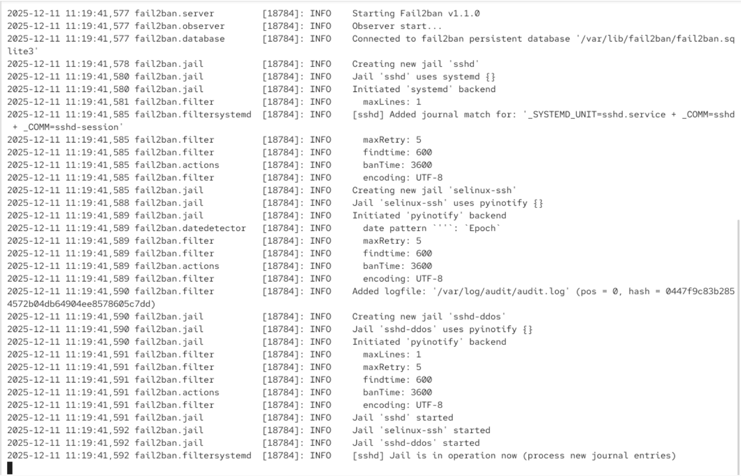
Включение защиты SSH



```
[DEFAULT]
bantime = 3600

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

:contentReferenceoaicite:3

Запуск jail-ов SSH

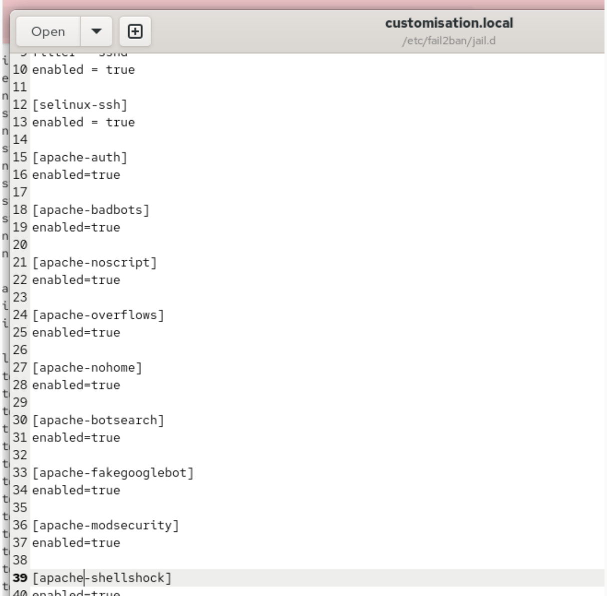


```
2025-12-11 11:19:41,577 fail2ban.server         [18784]: INFO    Starting Fail2ban v1.1.0
2025-12-11 11:19:41,577 fail2ban.observer       [18784]: INFO    Observer start...
2025-12-11 11:19:41,577 fail2ban.database       [18784]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sq
lite3'
2025-12-11 11:19:41,578 fail2ban.jail           [18784]: INFO    Creating new jail 'sshd'
2025-12-11 11:19:41,580 fail2ban.jail           [18784]: INFO    Jail 'sshd' uses systemd {}
2025-12-11 11:19:41,580 fail2ban.jail           [18784]: INFO    Initiated 'systemd' backend
2025-12-11 11:19:41,581 fail2ban.filter         [18784]: INFO      maxLines: 1
2025-12-11 11:19:41,585 fail2ban.filtersystemd  [18784]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd
 + _COMM=sshd-session'
2025-12-11 11:19:41,585 fail2ban.filter         [18784]: INFO      maxRetry: 5
2025-12-11 11:19:41,585 fail2ban.filter         [18784]: INFO      findtime: 600
2025-12-11 11:19:41,585 fail2ban.actions        [18784]: INFO      banTime: 3600
2025-12-11 11:19:41,585 fail2ban.filter         [18784]: INFO      encoding: UTF-8
2025-12-11 11:19:41,585 fail2ban.jail           [18784]: INFO    Creating new jail 'selinux-ssh'
2025-12-11 11:19:41,588 fail2ban.jail           [18784]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2025-12-11 11:19:41,589 fail2ban.jail           [18784]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:19:41,589 fail2ban.datedetector   [18784]: INFO      date pattern `''`: `Epoch`
2025-12-11 11:19:41,589 fail2ban.filter         [18784]: INFO      maxRetry: 5
2025-12-11 11:19:41,589 fail2ban.filter         [18784]: INFO      findtime: 600
2025-12-11 11:19:41,589 fail2ban.actions        [18784]: INFO      banTime: 3600
2025-12-11 11:19:41,589 fail2ban.filter         [18784]: INFO      encoding: UTF-8
2025-12-11 11:19:41,590 fail2ban.filter         [18784]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 0447f9c83b285
4572b04db64904ee8578605c7dd)
2025-12-11 11:19:41,590 fail2ban.jail           [18784]: INFO    Creating new jail 'sshd-ddos'
2025-12-11 11:19:41,590 fail2ban.jail           [18784]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:19:41,590 fail2ban.jail           [18784]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:19:41,591 fail2ban.filter         [18784]: INFO      maxLines: 1
2025-12-11 11:19:41,591 fail2ban.filter         [18784]: INFO      maxRetry: 5
2025-12-11 11:19:41,591 fail2ban.filter         [18784]: INFO      findtime: 600
2025-12-11 11:19:41,591 fail2ban.actions        [18784]: INFO      banTime: 3600
2025-12-11 11:19:41,591 fail2ban.filter         [18784]: INFO      encoding: UTF-8
2025-12-11 11:19:41,591 fail2ban.jail           [18784]: INFO    Jail 'sshd' started
2025-12-11 11:19:41,592 fail2ban.jail           [18784]: INFO    Jail 'selinux-ssh' started
2025-12-11 11:19:41,592 fail2ban.jail           [18784]: INFO    Jail 'sshd-ddos' started
2025-12-11 11:19:41,592 fail2ban.filtersystemd  [18784]: INFO    [sshd] Jail is in operation now (process new journal entries)
▌
```

:contentReferenceoaicite:4

Защита HTTP-служб

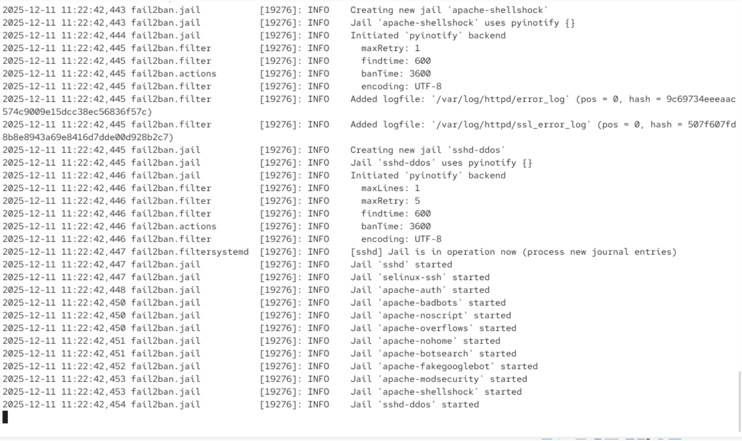
Включение HTTP jail-ов



```
filter = sshd
enabled = true

[selinux-ssh]
enabled = true

[apache-auth]
enabled=true

[apache-badbots]
enabled=true

[apache-noscript]
enabled=true

[apache-overflows]
enabled=true

[apache-nohome]
enabled=true

[apache-botsearch]
enabled=true

[apache-fakegooglebot]
enabled=true

[apache-modsecurity]
enabled=true

[apache-shellshock]
enabled=true
```

:contentReferenceoaicite:5

Запуск HTTP jail-ов

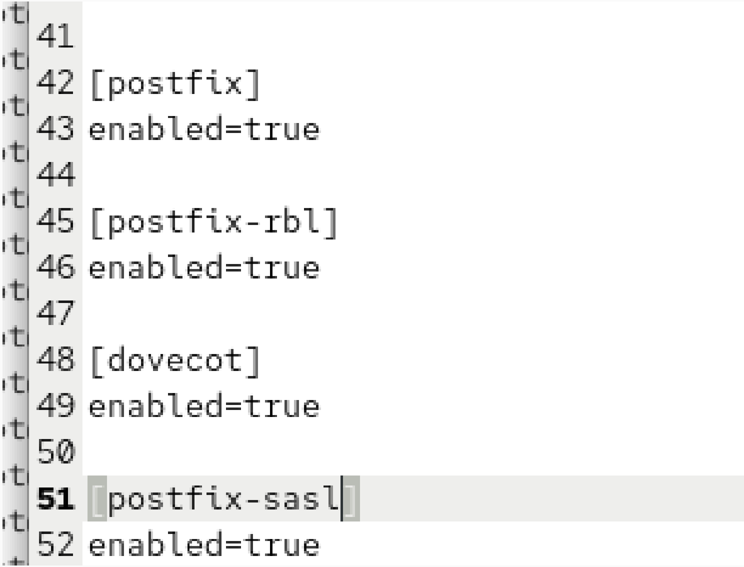


```
2025-12-11 11:22:42,443 fail2ban.jail          [19276]: INFO    Creating new jail 'apache-shellshock'
2025-12-11 11:22:42,443 fail2ban.jail          [19276]: INFO    Jail 'apache-shellshock' uses pyinotify {}
2025-12-11 11:22:42,444 fail2ban.jail          [19276]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:22:42,445 fail2ban.filter        [19276]: INFO      maxRetry: 1
2025-12-11 11:22:42,445 fail2ban.filter        [19276]: INFO      findtime: 600
2025-12-11 11:22:42,445 fail2ban.actions       [19276]: INFO      banTime: 3600
2025-12-11 11:22:42,445 fail2ban.filter        [19276]: INFO      encoding: UTF-8
2025-12-11 11:22:42,445 fail2ban.filter        [19276]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 9c69734eeeaac
574c9009e15dcc38ec56836f57c)
2025-12-11 11:22:42,445 fail2ban.filter        [19276]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 507f607fd
8b8e8943a69e8416d7dde00d928b2c7)
2025-12-11 11:22:42,445 fail2ban.jail          [19276]: INFO    Creating new jail 'sshd-ddos'
2025-12-11 11:22:42,445 fail2ban.jail          [19276]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:22:42,446 fail2ban.jail          [19276]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:22:42,446 fail2ban.filter        [19276]: INFO      maxLines: 1
2025-12-11 11:22:42,446 fail2ban.filter        [19276]: INFO      maxRetry: 5
2025-12-11 11:22:42,446 fail2ban.filter        [19276]: INFO      findtime: 600
2025-12-11 11:22:42,446 fail2ban.actions       [19276]: INFO      banTime: 3600
2025-12-11 11:22:42,446 fail2ban.filter        [19276]: INFO      encoding: UTF-8
2025-12-11 11:22:42,447 fail2ban.filtersystemd [19276]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:22:42,447 fail2ban.jail          [19276]: INFO    Jail 'sshd' started
2025-12-11 11:22:42,447 fail2ban.jail          [19276]: INFO    Jail 'selinux-ssh' started
2025-12-11 11:22:42,448 fail2ban.jail          [19276]: INFO    Jail 'apache-auth' started
2025-12-11 11:22:42,450 fail2ban.jail          [19276]: INFO    Jail 'apache-badbots' started
2025-12-11 11:22:42,450 fail2ban.jail          [19276]: INFO    Jail 'apache-noscript' started
2025-12-11 11:22:42,450 fail2ban.jail          [19276]: INFO    Jail 'apache-overflows' started
2025-12-11 11:22:42,451 fail2ban.jail          [19276]: INFO    Jail 'apache-nohome' started
2025-12-11 11:22:42,451 fail2ban.jail          [19276]: INFO    Jail 'apache-botsearch' started
2025-12-11 11:22:42,452 fail2ban.jail          [19276]: INFO    Jail 'apache-fakegooglebot' started
2025-12-11 11:22:42,453 fail2ban.jail          [19276]: INFO    Jail 'apache-modsecurity' started
2025-12-11 11:22:42,453 fail2ban.jail          [19276]: INFO    Jail 'apache-shellshock' started
2025-12-11 11:22:42,454 fail2ban.jail          [19276]: INFO    Jail 'sshd-ddos' started
█
```

:contentReferenceoaicite:6

Защита почтовых служб

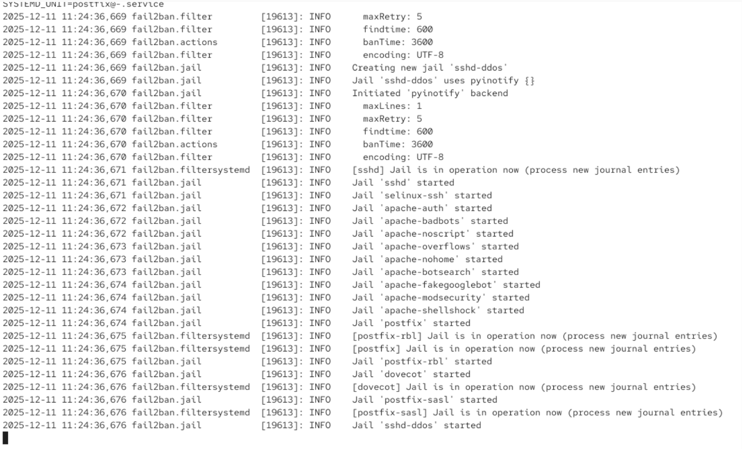
Включение почтовых jail-ов



```

[postfix]
enabled=true

[postfix-rbl]
enabled=true

[dovecot]
enabled=true

[postfix-sasl]
enabled=true
```

:contentReferenceoaicite:7

Запуск почтовых jail-ов

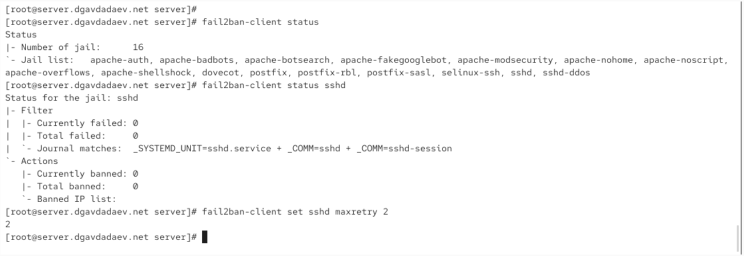


```
SYSTEMD_UNIT=postfix@-.service
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      maxRetry: 5
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      findtime: 600
2025-12-11 11:24:36,669 fail2ban.actions        [19613]: INFO      banTime: 3600
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      encoding: UTF-8
2025-12-11 11:24:36,669 fail2ban.jail           [19613]: INFO    Creating new jail 'sshd-ddos'
2025-12-11 11:24:36,669 fail2ban.jail           [19613]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:24:36,670 fail2ban.jail           [19613]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      maxLines: 1
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      maxRetry: 5
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      findtime: 600
2025-12-11 11:24:36,670 fail2ban.actions        [19613]: INFO      banTime: 3600
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      encoding: UTF-8
2025-12-11 11:24:36,671 fail2ban.filtersystemd  [19613]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,671 fail2ban.jail           [19613]: INFO    Jail 'sshd' started
2025-12-11 11:24:36,671 fail2ban.jail           [19613]: INFO    Jail 'selinux-ssh' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-auth' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-badbots' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-noscript' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-overflows' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-nohome' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-botsearch' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-fakegooglebot' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-modsecurity' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-shellshock' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'postfix' started
2025-12-11 11:24:36,675 fail2ban.filtersystemd  [19613]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.filtersystemd  [19613]: INFO    [postfix] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.jail           [19613]: INFO    Jail 'postfix-rbl' started
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'dovecot' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd  [19613]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'postfix-sasl' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd  [19613]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'sshd-ddos' started
█
```

:contentReferenceoaicite:8

Проверка защиты SSH

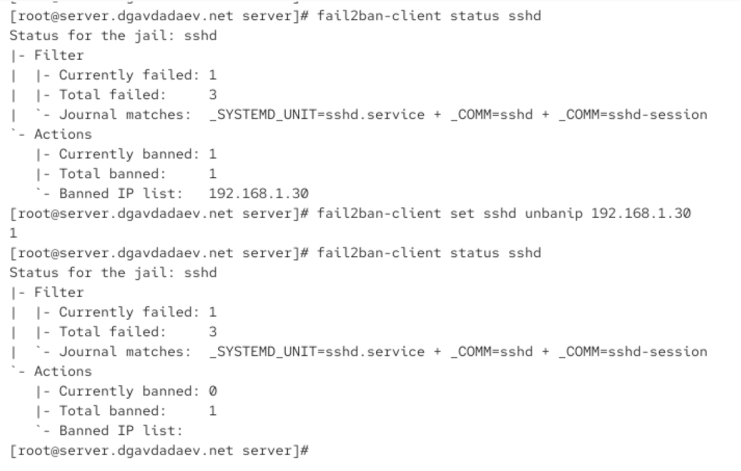
Общий статус Fail2ban



```
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript,
apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.dgavdadaev.net server]# fail2ban-client set sshd maxretry 2
2
[root@server.dgavdadaev.net server]#
```

:contentReferenceoaicite:9

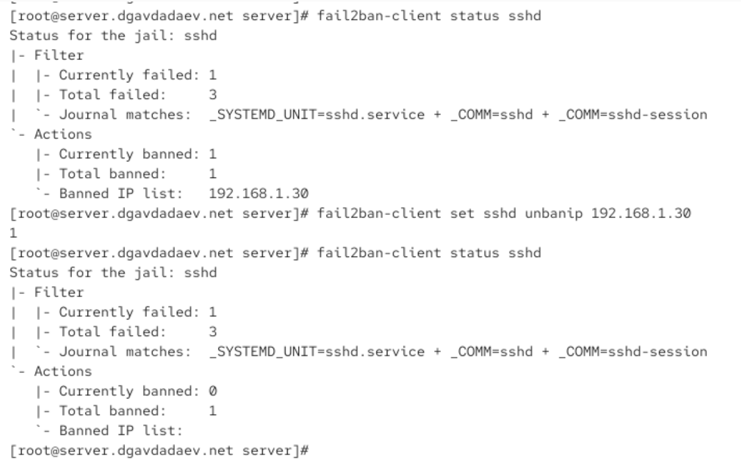
Блокировка при ошибке входа



```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

:contentReferenceoaicite:10

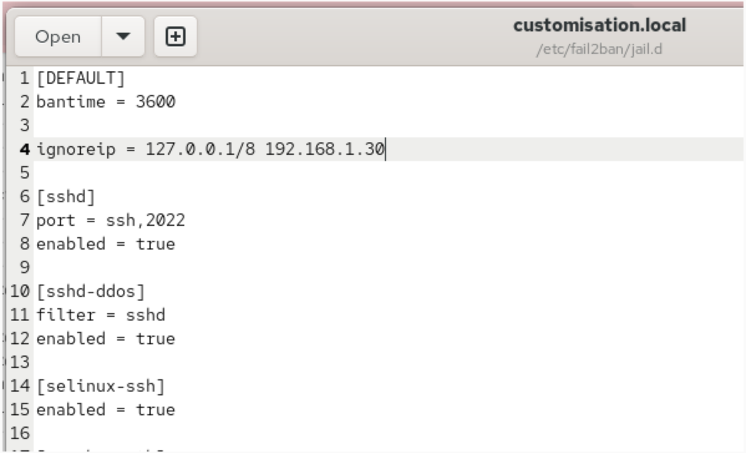
Разблокировка IP



```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

:contentReferenceoaicite:11

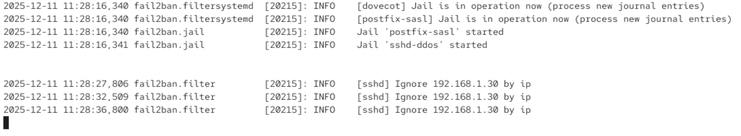
Добавление IP в ignoreip



```
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.30

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true

```

:contentReferenceoaicite:12

Проверка игнорирования IP



```
2025-12-11 11:28:16,340 fail2ban.filtersystemd  [20215]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:28:16,340 fail2ban.filtersystemd  [20215]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:28:16,340 fail2ban.jail           [20215]: INFO    Jail 'postfix-sasl' started
2025-12-11 11:28:16,341 fail2ban.jail           [20215]: INFO    Jail 'sshd-ddos' started


2025-12-11 11:28:27,806 fail2ban.filter         [20215]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:28:32,509 fail2ban.filter         [20215]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:28:36,800 fail2ban.filter         [20215]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

:contentReferenceoaicite:13

Вывод

Основные результаты

- Настроена защита SSH, HTTP и почтовых служб
- Проверена блокировка и разблокировка IP
- Настроен механизм ignoreip
- Подготовлен provisioning Fail2ban
- Fail2ban успешно защищает сервер от brute-force атак